

\$1 Billion Hotel Chain Manages Cyber Risk Posture Across Hotels with SAFE

INDUSTRY

Hospitality

RESULTS

- Security visibility into technology stack across the organization
- Factor People, policies, technology, cybersecurity products, and third party risk posture to generate overall risk posture
- Visibility across all hotels with a quantified digital risk score

CHALLENGES

- Remote working users not connected to the organization central network
- Human-intensive operations
- No visibility across all hotels to ensure security of customer PII data

THE NEED

The requirement was to monitor the cyber risk posture of the distributed infrastructure across all the hotels and manage the PII data of customers. The primary challenge was to enable CISOs to see the security posture across all the endpoints and servers across all the locations.

ON-GROUND EXECUTION CHALLENGES

Prior to SAFE, the organization didn't have a way to monitor the security posture of all the distributed infrastructure via SAFE score per hotel. Business nature demands users to travel, hence remote users would not be connecting to the organization network all the time. The absence of visibility into the users systems, hotel's systems across multiple geo blocked organization visualising and managing the security of PII data of customers.

BRING RIGHT VISIBILITY WITH SAFE

SAFE, is an enterprise-class, unified, and real-time Cyber Risk Quantification (CRQ) platform that offers a comprehensive solution, by taking into account both technical and business aspects, to arrive at informed and prioritised decision making. SAFE has a unique assessment approach across five threat vectors concerning organisations, namely People, Policy, Technology, Cybersecurity Products, and Third-parties. SAFE helped the organization with the following unique capabilities:

1. Asset grouping as per business requirements
2. Score per asset, per group
3. Remediation guidelines in SAFE to improve security posture
4. Continuous assessment and monitoring of IT assets on-cloud and on-prem
5. Actionable insights to identify most critical vulnerabilities to prioritize patching

1 SCORE PER ASSET, PER GROUP

SAFE generates a score (SAFE score) per asset based on the assessments performed by SAFE and factoring the inputs received from integrations with other tools. These assets can be further clubbed into an asset group per business unit or per application to factor the security posture of all the underlying assets such as servers, databases, middlewares, etc. This way of risk quantification helps organization in taking the right decision especially during the mission critical go-lives. The organization follows a policy of making sure that the overall SAFE score of a mission critical application is 3.5+ with 0 Critical or High vulnerabilities that could cause any business impact.

2 ASSET GROUPING AS PER BUSINESS REQUIREMENTS

SAFE provides organization with a consolidated view of SAFE score of various departments in a single widget. Any new business unit can be onboarded easily in SAFE and can be continuously monitored. Each Business Unit has been assigned a priority score and according to the delta change in its value, SAFE sends actionable alert to the asset group owner and/or concerned authorities in form of an email or system generated telephonic call.

3 REMEDIATION GUIDELINES IN SAFE TO IMPROVE SECURITY POSTURE

SAFE not only tells you what and how big the problem is, but it also walks you through the remediation and how it will impact your organization. The organization leverages SAFE to remediate the most critical gaps that may make your company the next headline in the newspaper. It guides you to reach the desired SAFE score according to your plan.

4 CONTINUOUS ASSESSMENT AND MONITORING OF IT ASSETS ON-CLOUD AND ON-PREM

SAFE can be deployed on-prem or cloud, and can be used as a single and the only platform in your organization to track your cybersecurity posture across all verticals. Org used SAFE to gain 360 degree view with fully automated configuration assessment performed natively and vulnerability management performed through integrations across their IT stack. SAFE supports more than 80 technology solutions across 11 verticals ranging from endpoints, databases to cloud services. SAFE further provides an execution plan to reach the desired SAFE score via actionable insights.

5 ACTIONABLE INSIGHTS TO IDENTIFY MOST CRITICAL VULNERABILITIES TO PRIORITIZE PATCHING

SAFE provides a prioritization matrix, which allows users to get visibility into the high-risk vulnerabilities in their landscape to fix or de-prioritize the gaps. SAFE also takes the Vulnerability based Risk management approach by giving insights on TSAR Vulnerabilities which are high-risk vulnerabilities that may have a publicly available exploit or determined as such by subject matter experts at Lucideus.

SAFE helps organizations measure and mitigate enterprise-wide cyber risk in real-time using its AI Enabled SAFE Platform by aggregating automated signals across people, process and technology to predict the breach likelihood (as SAFE Score) of an organization

USA (HQ)

Stanford Research Park
3260 Hillview Avenue
Palo Alto, CA 94304

INDIA

Lucideus House
Plot No 15, Okhla Phase III
New Delhi, 110020

\$1 Billion Hotel Chain Manages Cyber Risk Posture Across Hotels with SAFE

INDUSTRY

Hospitality

RESULTS

- Security visibility into technology stack across the organization
- Factor People, policies, technology, cybersecurity products, and third party risk posture to generate overall risk posture
- Visibility across all hotels with a quantified digital risk score

CHALLENGES

- Remote working users were not connected to the organization's central network
- Human-intensive operations
- No visibility across all hotels to ensure security of customer PII data

THE NEED

To monitor the cyber risk posture of the distributed infrastructure across all the hotels and manage the PII data of customers. The primary challenge was to enable CISOs to view the security posture of all the endpoints and servers across all the locations.

ON-GROUND EXECUTION CHALLENGES

The hotel didn't have a method to monitor the security posture of their distributed infrastructure. The nature of this industry is such that it requires travel. As a consequence remote users would not be connecting to the organization's native network. The absence of visibility into the user's devices in the hotel's systems across multiple geographies, reduced visualisation and made it difficult to secure the PII data of customers.

BRING RIGHT VISIBILITY WITH SAFE

SAFE is an enterprise-class, unified, and real-time Digital Business Risk Quantification (CRQ) platform which offers a comprehensive solution by taking into account both technical and business aspects and gives informed, prioritised insights. With its unique assessment approach across five threat vectors concerning organisations - People, Policy, Technology, Cybersecurity Products, and Third-parties - SAFE helped this organization with the following:

1. Asset grouping as per business requirements
2. Score per asset, per group
3. Remediation guidelines in SAFE to improve security posture
4. Continuous assessment and monitoring of IT assets on-cloud and on-prem
5. Actionable insights to identify most critical vulnerabilities to prioritize patching

1 SCORE PER ASSET, PER GROUP

SAFE generates a score (SAFE score) per asset based on the assessments it has performed, and by factoring the inputs received from integrations with other tools. These assets can be further clubbed into asset groups per business unit or per application to factor the security posture of all the underlying assets such as servers, databases, middlewares, etc. This means of business risk quantification helps the organization in taking the correct decision, especially during the mission critical go-lives. This organization follows a policy of making sure that the overall SAFE score of a mission critical application is 3.5+ with 0 Critical or High vulnerabilities that could cause any business impact.

2 ASSET GROUPING AS PER BUSINESS REQUIREMENTS

SAFE provides this organization with a consolidated view of SAFE score across departments through a single widget. Any new business unit can be on-boarded easily and be continuously monitored. Each Business Unit has been assigned a priority score and according to the delta change in its value, SAFE sends actionable alerts to the asset group owner and/ or concerned authorities in form of an email or system generated telephonic call.

3 REMEDIATION GUIDELINES IN SAFE TO IMPROVE SECURITY POSTURE

SAFE not only tells you what and how big the problem is, but it also walks you through how it will impact your organization & the remediation. It guides them to reach the desired SAFE score according to their plan. This organization leverages SAFE to remediate the most critical gaps that may make your company grab the next headline for the wrong reasons.

4 CONTINUOUS ASSESSMENT AND MONITORING OF IT ASSETS ON-CLOUD AND ON-PREM

SAFE can be deployed on-prem or cloud, and can be used as a single and the only platform in your organization to track your cybersecurity posture across all verticals. The organization used SAFE to gain 360 degree view with fully automated configuration assessment performed natively and vulnerability management performed through integrations across their IT stack. SAFE supports more than 80 technology solutions across 11 verticals ranging from endpoints, databases to cloud services. SAFE further provides an execution plan to reach the desired SAFE score via actionable insights.

5 ACTIONABLE INSIGHTS TO IDENTIFY MOST CRITICAL VULNERABILITIES TO PRIORITIZE PATCHING

SAFE provides a prioritization matrix, which allows users to get visibility into the high-risk vulnerabilities in their landscape to fix or de-prioritize the gaps. SAFE also takes the Vulnerability-based Risk management approach by giving insights on high-risk TSAR Vulnerabilities that may have a publicly available exploit or determined as such by subject matter experts at Lucideus.

SAFE helps organizations measure and mitigate enterprise-wide cyber risk in real-time using its AI Enabled SAFE Platform by aggregating automated signals across people, process and technology to predict the breach likelihood (as SAFE Score) of an organization

USA (HQ)

Stanford Research Park
3260 Hillview Avenue
Palo Alto, CA 94304

INDIA

Lucideus House
Plot No 15, Okhla Phase III
New Delhi, 110020